Victim Support through Alignment of Remedies

ViSAR

Quality Management Concept

Milestone 1

ViSAR *– Victim Support through alignment of Remedies; GA-No.: 101160451*
This project is co-funded by the European Commission, Directorate-General for Migration and Home Affairs under Grant Agreement number: 101038761.

Table of Contents

1. Change Control

1.1 Document Properties

Milestone No.		1	
Work Package No.	WP 1	**Work Package Title**	Project-, Process- and Quality-Management
Author/s		Court of Appeal Team - Venezia	
Contributor/s		MA Sarah Holland-Kunkel (HfÖV) Trygve Ben Holland (HfÖV) Marina Caneva (CoA) Sergio Bianchi (AGF)	
Name		Quality Management Concept	
Date		16th November 2024	

1.2 Revision History

Version	Date	Comments
1.0	16th November 2024	First version shared with partners for comments and additions.
2-0	10/12/2024	Version revised by AGF
3.0	12/12/2024	Version revised by CIPOS
4,0	22/12/2024	Definitive version by the coordinator

1.3 Table of Abbreviations and Acronyms

AFSJ	Area of Freedom, Security and Justice
Art.	Article
cf.	confer
CJEU	Court of Justice of the EU
CSO(s)	Civil Society Organisation(s)
CSP	Communication Strategy Plan
DCP	Dissemination and Communication Plan
ECHR	European Convention on Human Rights
EIGE	European Institute for Gender Equality
e.g.	exempli gratia
EU	European Union
GA	Grant Agreement
i.e.	id est
M	Milestone
No.	number
p.	page
para.	paragraph
PPM	Project and Process Management (function)
PPQM	Project-, Process-, and Quality Management
Rec.	Recital
TFEU	Treaty on the Functioning of the EU
WG(s)	Working Group(s)
WP(s)	Work Package(s)

2. Background

Project ViSAR facilitates effective and non-discriminatory access to justice for victims of crimes and redress, including by electronic means through promoting efficient criminal procedures with a victim-centred focus on the promotion of rights. ViSAR build on three main background elements: fragmented implementation of the Dir 2012/29 at member states levels; its specific application in cases of victims of domestic violence; and, finally, correlation with the EU Protection Order.

WP1 on Project-, Process- and Quality-Management aims, overall, at implementing project ViSAR according to the GA by planning, organising, securing, monitoring and managing the resources and work necessary to deliver specific project goals and objectives in an effective and efficient way (IPMA and PM2 Methodology).

Specifically, WP1 aims to

- undertake necessary central project and process management functions to support the project in meeting the objectives;
- keep the project schedule and to guarantee implementation of the work plan and the achievement of the project goals in time and within budget;
- administer the contract and project financial management;
- justify the project progress towards the European Commission;
- assure overall consistency and validated quality of the deliverables before submission to the European Commission;
- implement the management structure.

M1 focuses on the establishment of a Quality Management Concept throughout all project activities in order to ensure the compliance with EU ethical and fundamental rights principles and standards.

The Quality Management Concept report conducts and delivers assessments of the project activities with a focus on ethics and human rights, ensuring implementation of the key good governance attributes: transparency, responsibility, accountability,

participation, and responsiveness, for example, by defining and implement the Data Management Plan (DMP) and Data-Protection Concept (DPC).

The Quality Management Concept assesses, advises and raises (if applicable) concerns regarding any ethical issue to the ViSAR team.

3. Data Management and Data Protection

3.1 Data Description

3.1.1 Data Generation

On the one hand, ViSAR uses publicly available data, especially from literature, the press and websites of authorities, companies and CSOs in the framework of the Open Data Directive (**Directive (EU) 2019/1024**).

On the other hand, data from sources that are not generally accessible to the public are used, this applies in particular to:

(a) the analysis of files from law enforcement agencies, predominantly public prosecutors' offices, in line with the **Directive (EU) 2016/680 and the national regulations**;

(b) Judgements and acts from courts can be accessed for the reason that both the GDPR and the domestic provisions of the EU Member States apply.

Furthermore, data is obtained from semi-structured interviews with official users, CSO practitioners and officers of law enforcement and prosecutors. This data is subject to data consent, in line with GDPR.

These data are merged, cross-checked and analysed in terms of the research focus, resulting in new combined data sources and interpretations; in the case of the use of confidential data, underlying restrictions as to publication must be observed and is consequently only possible vis-à-vis the authorized institutions.

3.1.2 Re-using existing Data

Insofar as data already available are used, they are reused. However, no analyses in the sense of the ViSAR project are currently available. On the other hand, data from EU-

funded projects are reused on two levels: Case analyses from EU-funded projects in which the HfÖV and the other partners was or is are involved are used, and data from funded projects at German and EU level are used insofar as they have been made publicly accessible (e.g. in the EU's CORDIS system) or through cooperation agreements.

3.1.3 Data types and further processing

The data will be mainly textual, with graphical representations to a lesser extent. Further processing will take place at the respective secure premises and exclusively by project team members.

3.2 Documentation and Data Quality

3.2.1 Measures to ensure high data quality

On the one hand, data must be collected uniformly; for this purpose, the project team unanimously agrees on a data collection form tailored to the type of data envisaged. On the other hand, data must be analysed in a uniform manner, so that a corresponding decision must also be made in this regard. Regardless of the type of data to be collected or analysed, a data management officer is appointed from within the project team, who is supported by an external data officer. With regard to the external representative, the data itself may not be disclosed, shown, handed over or made accessible in any other way, but only a given problem may be discussed, in particular in order to find a solution.

3.2.2 Data Quality Controls

Data management is the responsibility of the data management officer with the right of veto, measured by the applicable detailed regulations of the funding decision; to ensure that the right of veto cannot be abused, its exercise is tied to the criterion of constructiveness: The veto must be accompanied by a proposal as to how an objectionable measure is to be designed differently and thus be capable of being decided (if such a proposal is not available or is not submitted immediately, the veto right does not apply).

3.2.3 Digital methods and tools required to use the data

This is data that can be processed with the usual applications and operating systems, e.g. Microsoft and Mac.

3.3 Storage and technical backup during the course of the project

3.3.1 Stored and backing-up Date during the project

Those consortium partners working behind authority's firewalls will maintain and secure any confidential data or data on natural persons referred to in project ViSAR. Data is stored on their secure servers.

3.3.2 Access and Usage Management

In addition to aspects outlined above on the security of sensitive data during the project and beyond, methods of pseudonymization will be applied in the case of personal data as soon as it is collected. This will apply in particular to data obtained from official files. Methods of pseudonymization within the framework of ViSAR are in accordance with the GDPR and Art. 2 No. 7 of the EU Open Data Directive, so that the protection of sensitive data is not waived. Methods of pseudonymization within the framework of the project therefore refer primarily to the final de-identification of such data that would allow conclusions to be drawn about persons at the time of data collection within the framework of file analyses. The same applies in the case of expert discussions with representatives of the public administration, organised civil society and companies, in case they don't provide the consent.

This applies to analyses of data as well as to publications that are realised in unanimous agreement within the project team. At the beginning of the project, a corresponding data management and use strategy must be unanimously and bindingly adopted by the project team; this must be accompanied by a data protection instruction to be signed by the project team members.

3.4 Legal obligations and framework conditions

3.4.1 Legal particularities in dealing with research data

The EU's Open Data Directive strategy must be considered as to any security-clearance related documents of the law enforcement authorities. According to the Directive, research data are "documents in digital form which are not scientific publications and which are collected or generated in the course of scientific research activities and used as evidence in the research process or which are generally considered necessary in the research community for the validation of research findings and results".

The EU's JHA Directive – designed for the judiciary and the police – also do not apply to ViSAR, as is focuses on the use of data in law enforcement measures.

Effects/restrictions on publication/accessibility

Data to be used is generally not subject to any restrictions with regard to publication and accessibility; the exception to this is any sensitive related data, which may only be communicated in relation to the respective authority.

3.4.2 Aspects of use and copyright as well as ownership issues

The project team is entitled to equal shares of the data and findings obtained, and they may jointly and individually use them for the purposes of the project as defined in the grant decision.

3.4.3 Relevant codes and standards

There are numerous codices and topic-specific norms of relevance when putting to practice ViSAR. With a certain hierarchy, the following ones are to be adhered to strategically and operationally: The *DFG Framework*,[1] the *European Charter for Researchers*[2] along with the *German interpretation in the sphere of security and justice*,[3] the *Best*

Practices published by the *Leopoldina*,[4] and the *Code of Conduct* when commercial operators of the security sector are involved in research activities[5].

3.5 Data exchange and permanent accessibility of data

3.5.1 Data particularly suitable for subsequent use in other contexts

All data emerging from investigation files and comparable documents are of potential interest to third parties for further use in research in the field of justice/internal security.

[1] www.dfg.de/download/pdf/foerderung/rechtliche_rahmenbedingungen/gute_wissenschaftliche_praxis/kodex_gwp.

[2] https://euraxess.ec.europa.eu/sites/default/files/am509774cee_en_e4.pdf

[3] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:075:0067:0077:DE:PDF

[4] https://www.sicherheitsrelevante-forschung.org

[5] www.bdsw.de/der-bdsw/verhaltenskodex

3.5.2 Criteria to select research data for subsequent use by others

Data are to be selected on the basis of thematic criteria; relevant keywords here are victims' rights, family violence, domestic violence, gender, etc.. Within this nexus, all data, especially those obtained from interviews, surveys and file material, must be made accessible in pseudonymized form.

3.5.3 Archiving Data in a Suitable Infrastructure

Data is stored in pseudonymized form on the consortium partners' own secure server where is a landing page for ViSAR. Since data is pseudonymized, there are no legal retention periods to observe; data will also be made available to the public as soon as the respective (partial) evaluation has taken place and publication took place (e.g. Journal Articles) or consent is granted by the respective parties. To ensure that the data can be found, they will be deposited on project ViSAR's own data section of the public website and at the same time made available to the general public in common file formats.

3.6 Responsibilities and Resources

3.6.1 Responsible for the adequate handling of research data

Responsibility for adequate handling of research data lies with the respective WP Lead. The analytical handling, on the other hand, is basically the responsibility of the respective team members under the aegis of the PPQM.

3.6.2 Resources Necessary for Adequate Data Handling

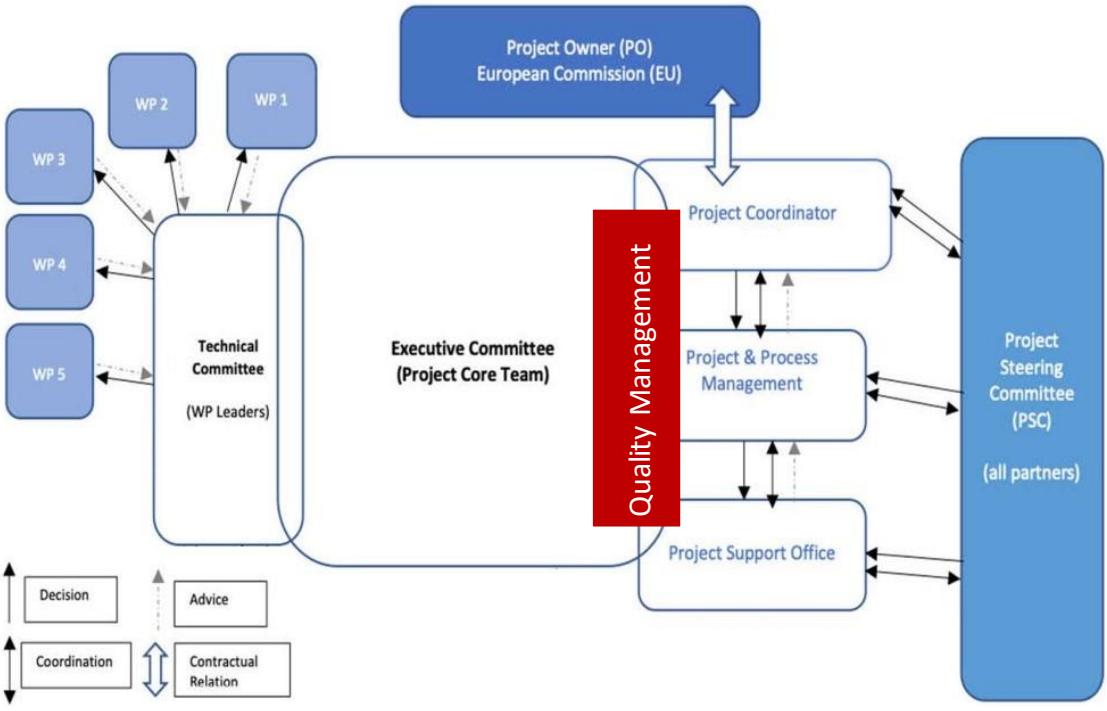
Maintenance of secured server structure is subject to the regular and standardised checks and updates inside the firewall-protected system architecture, conducted by the permanent IT staff of the consortium members. It follows that there are no additional and ViSAR-specific resources required (also not budget-related) to allow adequate handling of research data.

4. Establishing and Operating Quality Management

The underlying project proposal, now forming part of the GA, states on p. 28: "The quality management concept report is developed with the input of all the consortium members, reviewed and published on the project website."

4.1 Establishing the Quality Management

During the Kick-off Meeting in Athens on 31 October 2024 the quality management structure was adopted unanimously and amicably by the consortium team members (with two changes to the initial proposal).



4.2 Operating the Quality Management

Discussion of operating Quality Management found the following aspects and structure most suitable:

Project Steering Committee (PSC)

The PSC is chaired by the Project Coordinator (PC) and composed of the WP leaders. Tasks: ***a)*** monitor progress/achievements/expenditures, ***b)*** approve key documents, ***c)*** take key-decisions on significant issues likely to have impact on the project's/ team's capability to deliver on objectives, ***d)*** provide conflict resolution mechanisms on issues likely to have impact on medium/ long term actions or overall strategies, resources and achievement of objectives (though the decision-making envisages PSC members' consensus, in cases of doubt majority vote shall suffice), ***e)*** define plans to facilitate solving problems with potential effects on actions/strategies, ***f)*** supervise deliverables, data management and protection measures, use of (interim) results, ***g)*** prepare, if required, contract/agreement changes or amendments.

Project Coordinator (PC) and PPM

The PC oversee the normal course of project management, ***a)*** administration and resources coordination of resources, ***b)*** financial management, ***c)*** monitor/control compliance with & progress concerning the work plan, ***d)*** identify risks and define contingency plans, ***e)*** draft minutes/reports (Periodic/Final/Status Reports, Expenditure Statement), ***f)*** review/submission of deliverables, ***g)*** communication with the EC/team/third parties, ***h)*** organise plenary meetings and events. The PC is supported by the ***Project and Project Management (PPM)*** at operational level. The PPM oversees the project on a daily basis and takes responsibility to ensure delivery of high-quality results by the team. The PPM oversees progress and assesses potential risks concerning project's objectives. The PPM is assisted by the ***Project Support Office*** (PSO) where the different ***Coordinators*** and ***Officers*** – occasionally in distinct sub-boards – are gathered.

Law and Ethics Officer (LEO): Guides on project activities/adherence to EU provisions. S/He comprises representatives of end-user partners, Ethics Manager and experts from partner bodies who have experience in tracking ethics, privacy, data protection, and legislation. Specific role: ***a)*** Examine work plan continuously for ethical/legal questions, ***b)*** monitor/review deliverables where ethical questions may arise, ***c)*** monitor legal and ethical implications, ***d)*** propose solutions to legal/ethical questions of participants, ***e)*** ensure approval of ethical procedures.

Data Management and Protection Officer (DMPO): Guides on project activities/ adherence to the EU provisions. S/He is chaired by the LEO and comprises representatives of all shareholders. Role: ***a)*** continuously examine the work plan on data management questions, ***b)*** monitor/ review deliverables if data management questions arise, ***c)*** monitor privacy implications, ***d)*** solve data management questions, ***e)*** ensure approval of data management procedures.

Security Officer (SO): The SO represents the ***Security Advisory Board*** (SAB), formed of team members with extensive knowledge on security issues. The SO is in charge of managing such data and assessing sensitivity of the outputs (esp. publications, papers, press releases) to ensure compliance with regulatory issues and data protection concerns.

IPR and ***Innovation Officer*** (IPO): Handles transfer management to achieve aims and objectives as to uptake and outreach (medium term). Specific tasks: ***a)*** ensure protection of back-/front-end access rights for third parties, confidentiality agreements, ***b)*** analyse IPRs issues and advise on exploitation strategies (e.g. licensing, knowledge transfer), ***c)*** evaluate/approve joint exploitation/technology transfer actions.

Gender Officer (GO): The GO ensures that all activities are appropriately accounting for gender aspects during project implementation.

Civil Society Officer (CSO): Responsible to coordinate civic end users and prepare scenarios before/during validation phases. S/He ***a)*** facilitates inter-LEA communication, and civil society organisations, ***b)*** characterises scenarios for validation accor-

ding to end users involved and capabilities of developed solutionsc, ***c)*** monitors training courses for civil society involved in validation, ***d)*** ensures that end-users' expectations/needs are met to maximise impact, ***e)*** collects feedback on trial results, ***f)*** collaborates with DCO to promote cooperation with other bodies.

Dissemination & Communication Officer (DCO): oversees coordination of all dissemination and communication activities to ***a)*** channel team information to stake-holders and the general public, ***b)*** coordinates communication (all channels), ***c)*** furthers dissemination through participation (e.g. workshops, conferences, scientific journals), ***d)*** promotes collaboration with related projects, ***e)*** coordinate activities with WP leaders, ***f)*** contact stakeholders to participate in activities, ***g)*** reports to the PPM on deviations affecting results and/or objectives.

Technical Committee (TC)

The TC supports the PSC/PC as to questions on research/technical developments during the project. The TC is composed of the WP and esp. WG leaders. The TC is chaired by the Technical Manager (TM). The TM's function include ***a)*** management of dependencies between WG results, ***b)*** review and approve technical reports and deliverables, and resolution of technical issues, ***c)*** monitor the general scientific and technological community in those research areas tackled by the project to determine the state-of-the-art and industry evolution, ***d)*** monitor (potential for) cooperation with related projects, networks, and research communities.

5. Ethical Aspects of Relevance in Project ViSAR

The design of project ViSAR requires ethical considerations to a) research ethics; b) data protection, c) gender and non-discrimination, d) AI ethics, and e) compliance with EU values in EU AFSJ-related research.

5.1 Research Ethics

ViSAR is carried out in line with the highest ethical standards and the applicable EU, international and national law on ethical principles; the team commits itself to and ensure the respect of basic EU values within the meaning of ***Art. 2 TEU***. Additionally, the following research specific standards deriving from European and German best practices in the field of security- and justice-related projects are adhered to.[6]

5.2 Privacy and Data Protection

In principle, the project does not use individuals' data by any means; exemption: signed lists of participants to be disclosed to the European Commission only, handled in line with Reg. 2018/1725. Any other data are pseudonymized and processed within thelimits set out in Reg. (EU) 2016/679 and Dir (EU) 2016/680.

A project-specific Data Management Declaration is explained to participants in project events and signed individually. A Data Management Strategy (month 2) will be subject to on-going updating. The data protection concept comprises technical and factual measures and the control activities according to the applicable European legislation (Regulation 2016/679, Directive 2016/680, Regulation 2018/1725) These norms are to be respected within the team and whenever information are shared or disclosed with third parties, based on a data protection declaration.

[6] 1. www.dfg.de/download/pdf/foerderung/rechtliche_rahmenbedingungen/gute_wissenschaftliche_praxis/kodex_gwp.pdf; 2. https://euraxess.ec.europa.eu/sites/default/files/am509774cee_en_e4.pdf; 3. www.kowi.de/kowi/horizon-europe/horizon-europe2/weitere-aspekte/europaeische-charta-und-verhaltenskodex.aspx; 4. www.leopoldina.org/uploads/tx_leopublication/2014_06_DFG_Leopoldina_Wissenschaftsfreiheit _verantwortung_D.pdf; 5. www.bdsw.de/der-bdsw/verhaltenskodex

5.3 Gender and Non-Discrimination

Gender-related aspects and non-discriminatory approaches are subject to distinct procedural, organisational, managerial and institutional facets of mainstreaming in the framework of the ViSAR.

.

5.4 AI Ethics

As access to high quality data is an essential factor in building high quality justice and law enforcement services, any AI systems envisaged to be applied in the EU must comply with decisive EU provisions and initiatives, such as the EU Cybersecurity Strategy, the Digital Services Act and the Digital Markets Act, and the Data Governance Act. Hence, the AI-supported activities to be developed and applied in project ViSAR adheres to the EU's Coordinated Plan on Artificial Intelligence and the Proposal for a EU Regulation laying down harmonised rules on AI (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206).

5.5 EU Values Compliance

Compliance with EU values goes beyond the provisions of ***Art. 2 TEU*** according to which the EU itself (para 1) is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities; according to para 2, these values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail."

Art. 2 EUT identifies the fundamental values that constitute the essence of a democratic society – in its liberal European understanding – and declares them to be the EU's baseline (cf. Schimmelfennig, Frank, The EU: Promoting Liberal-Democracy through Membership Conditionality, pp. 106-126, in: Flockhart, Trine (ed.), Socializing Democratic Norms: The Role of International Organizations for the Construction of

Europe, Palgrave Macmillan, 2005). However, there is no definition of the concept of (liberal) democracy except for the electoral element. Consequently, ViSAR back-couples all its activities, measures and result outputs with human and fundamental rights enshrined in the CFR and ECHR.

In the course of implementing project ViSAR, also ***Art. 19 TFEU*** is of relevance, as any discrimination on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation is prohibited. This of high relevance for project ViSAR as the project's scope addresses at least the dimension of sexual orientation and sex, i.e. the gender-relevant elements.

Disclaimer

The content of this document represents the views of the author(s) only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Quality Management Concept

Milestone No. 1